Training-Free Coverless Multi-Image Steganography with Access Control

Minyeol Bae and Si-Hyeon Lee

School of EE, KAIST, South Korea

43rd International Conference on Machine Learning

Image Steganography

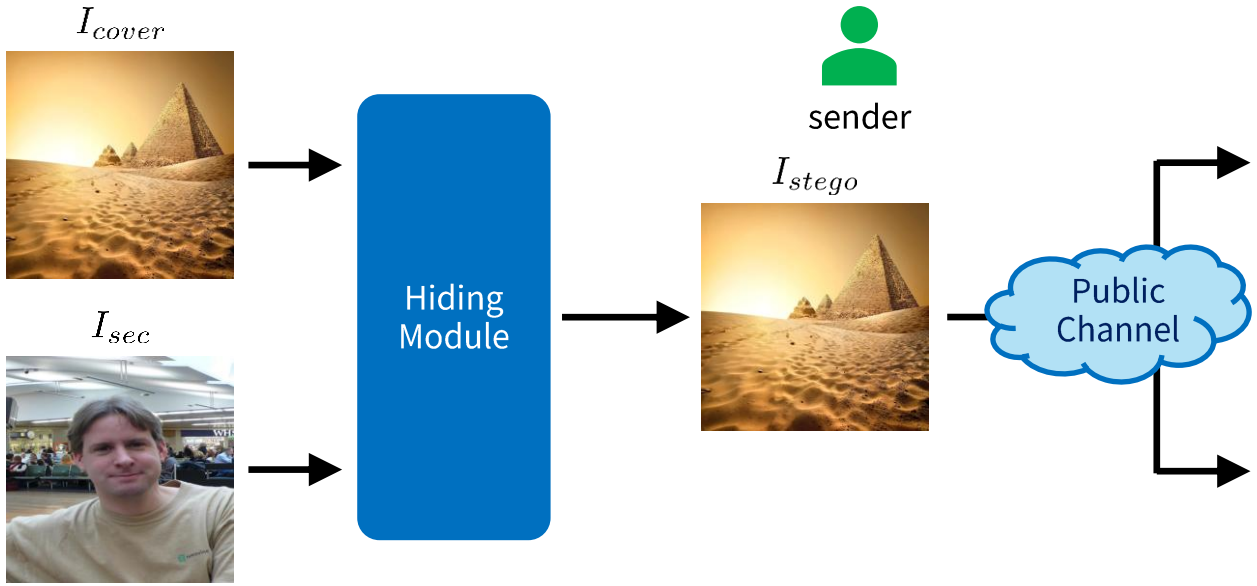


Image Steganography

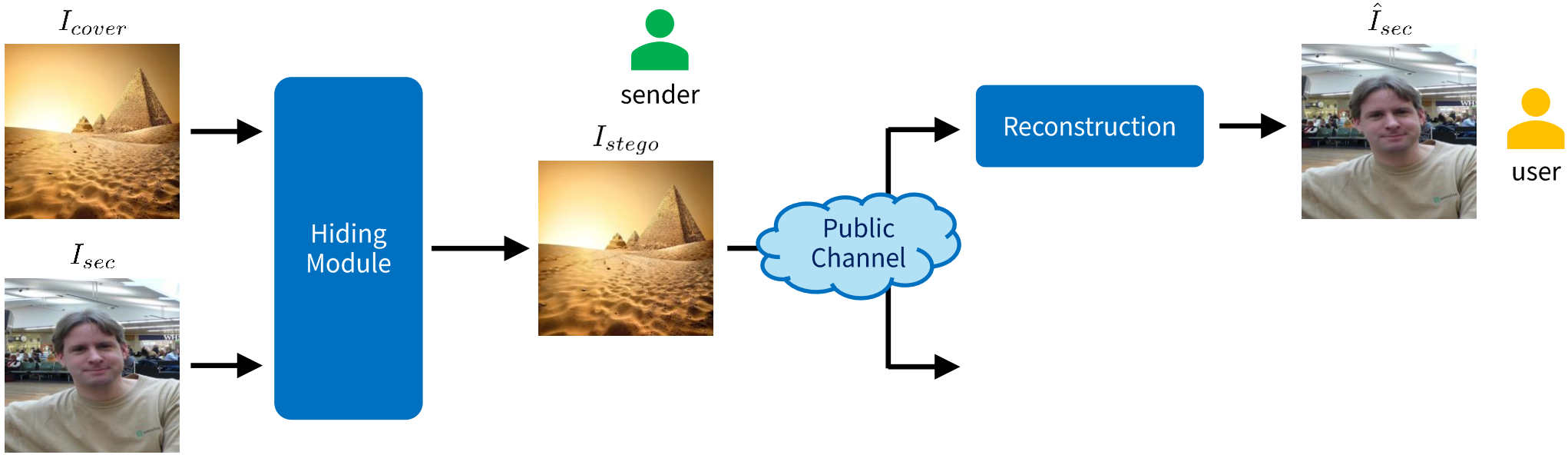
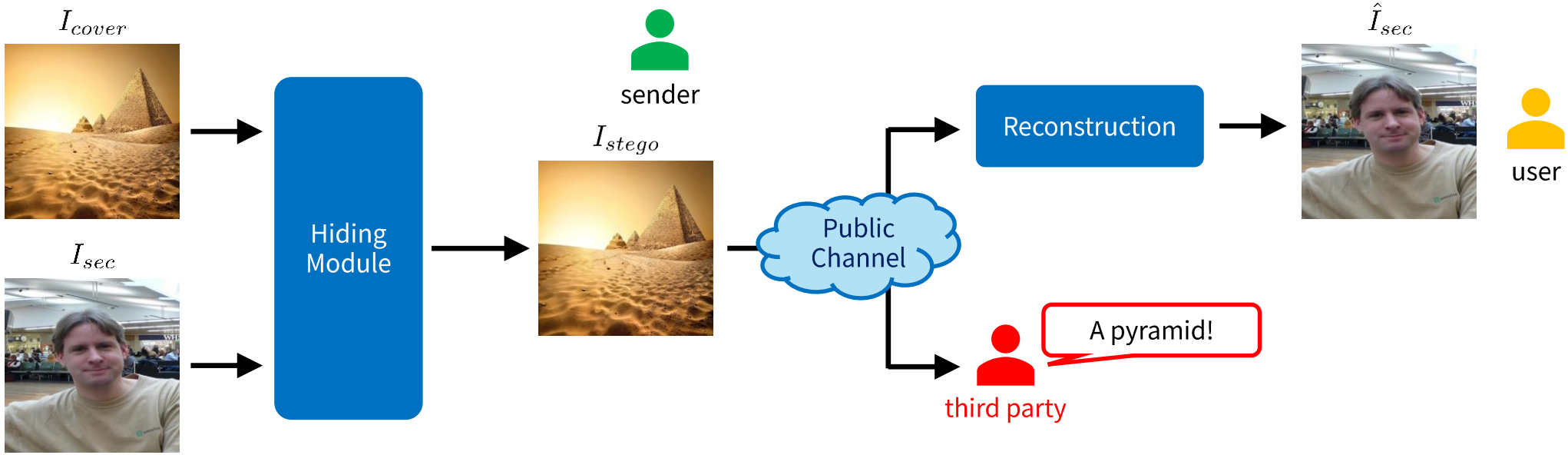
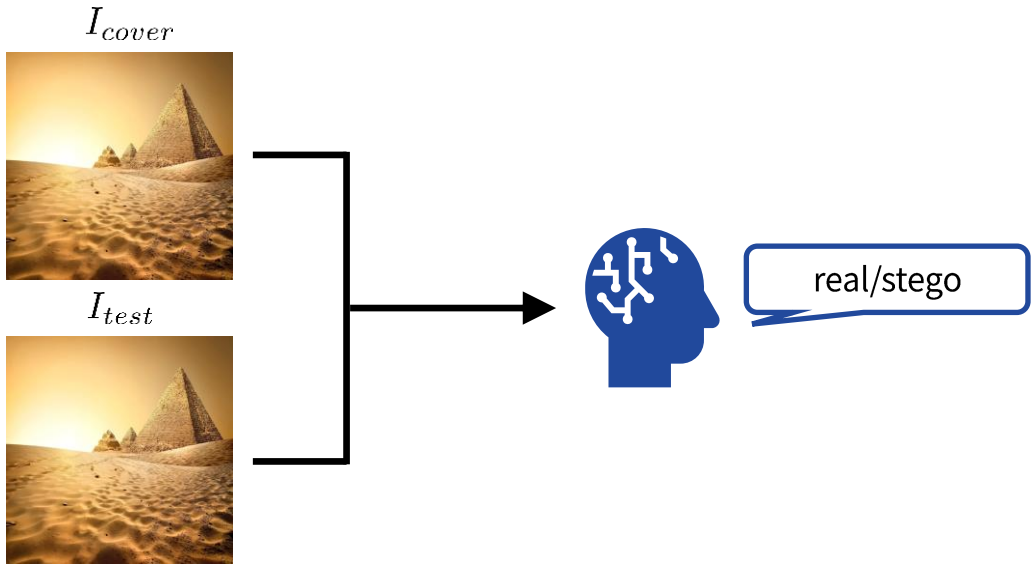


Image Steganography



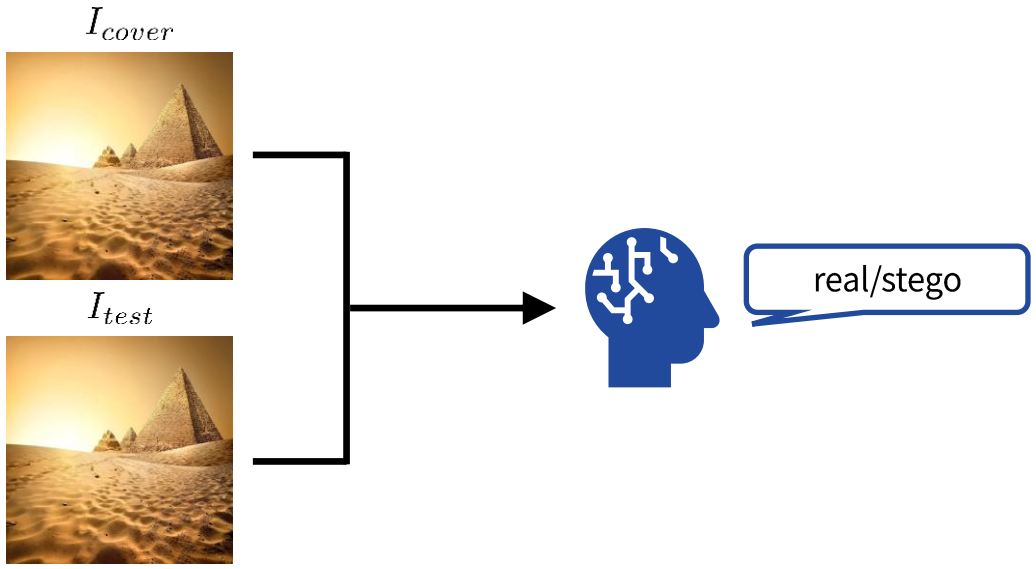
Challenges

Challenge 1: Security

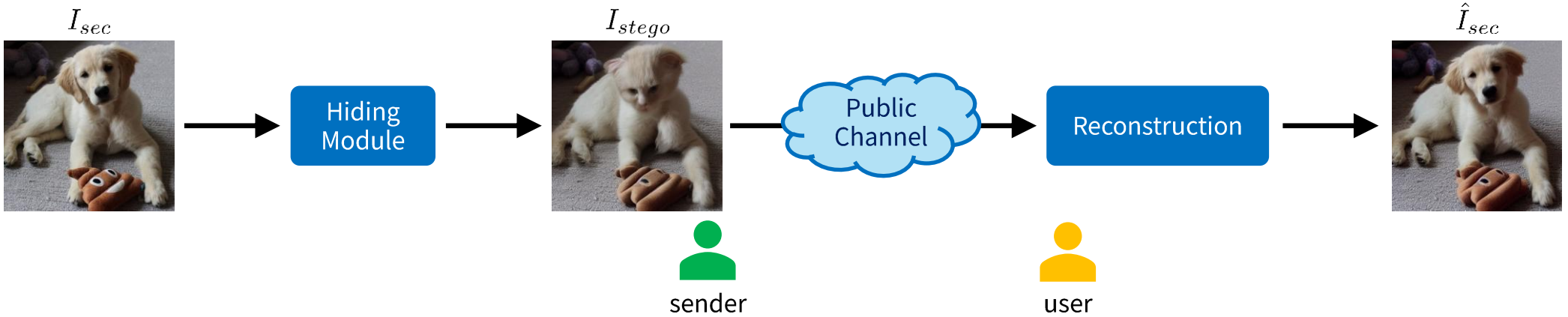


Challenges

Challenge 1: Security



Solution 1: Coverless Image Steganography (CIS)



Challenges

Challenge 2: Capacity

- Existing training-free CIS methods mainly support hiding only a **single** image.
- Training generative models is **resource-intensive**.

Challenges

Challenge 2: Capacity

- Existing training-free CIS methods mainly support hiding only a **single** image.
- Training generative models is **resource-intensive**.

Challenge 3: Access Control

- In multi-image hiding scenarios, each secret image may be intended for a distinct receiver.

Challenges

Challenge 2: Capacity

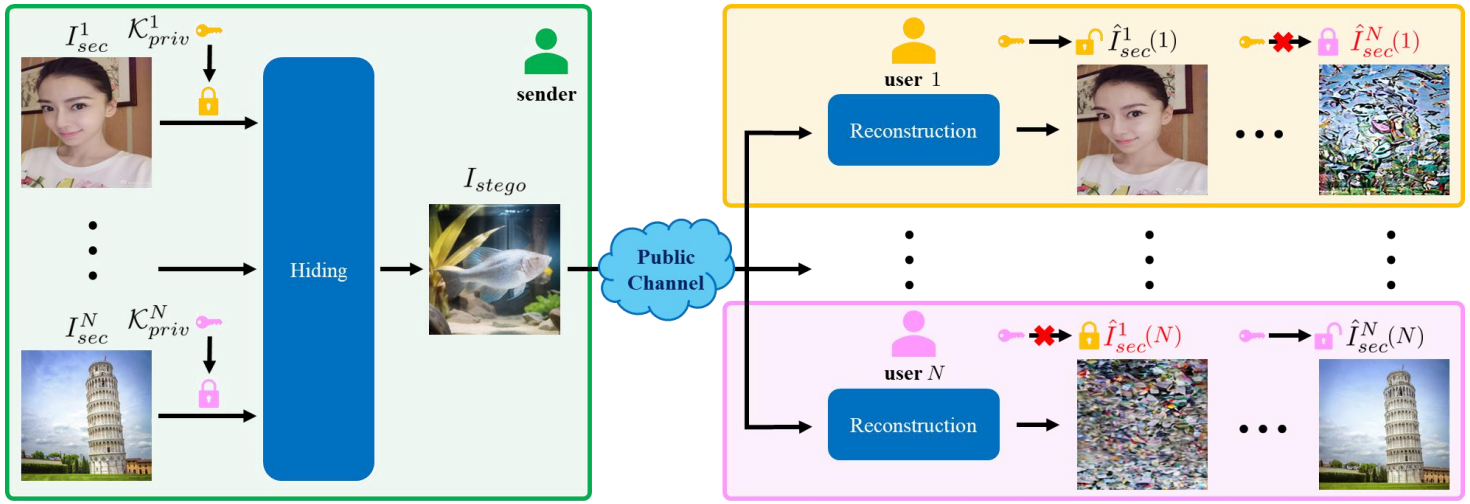
- Existing training-free CIS methods mainly support hiding only a **single** image.
- Training generative models is **resource-intensive**.

Challenge 3: Access Control

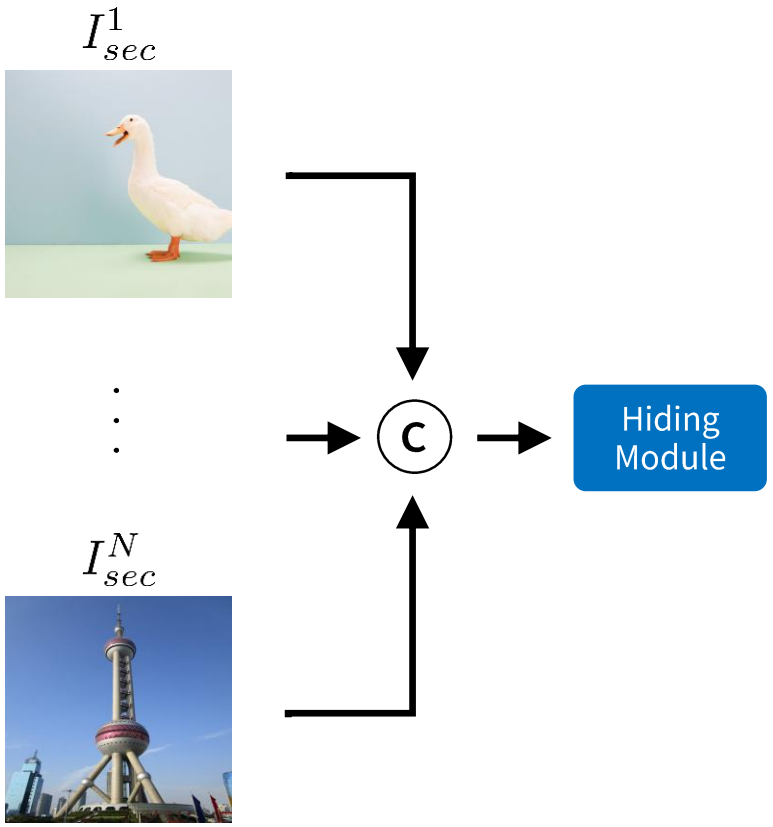
- In multi-image hiding scenarios, each secret image may be intended for a distinct receiver.

Our Contribution

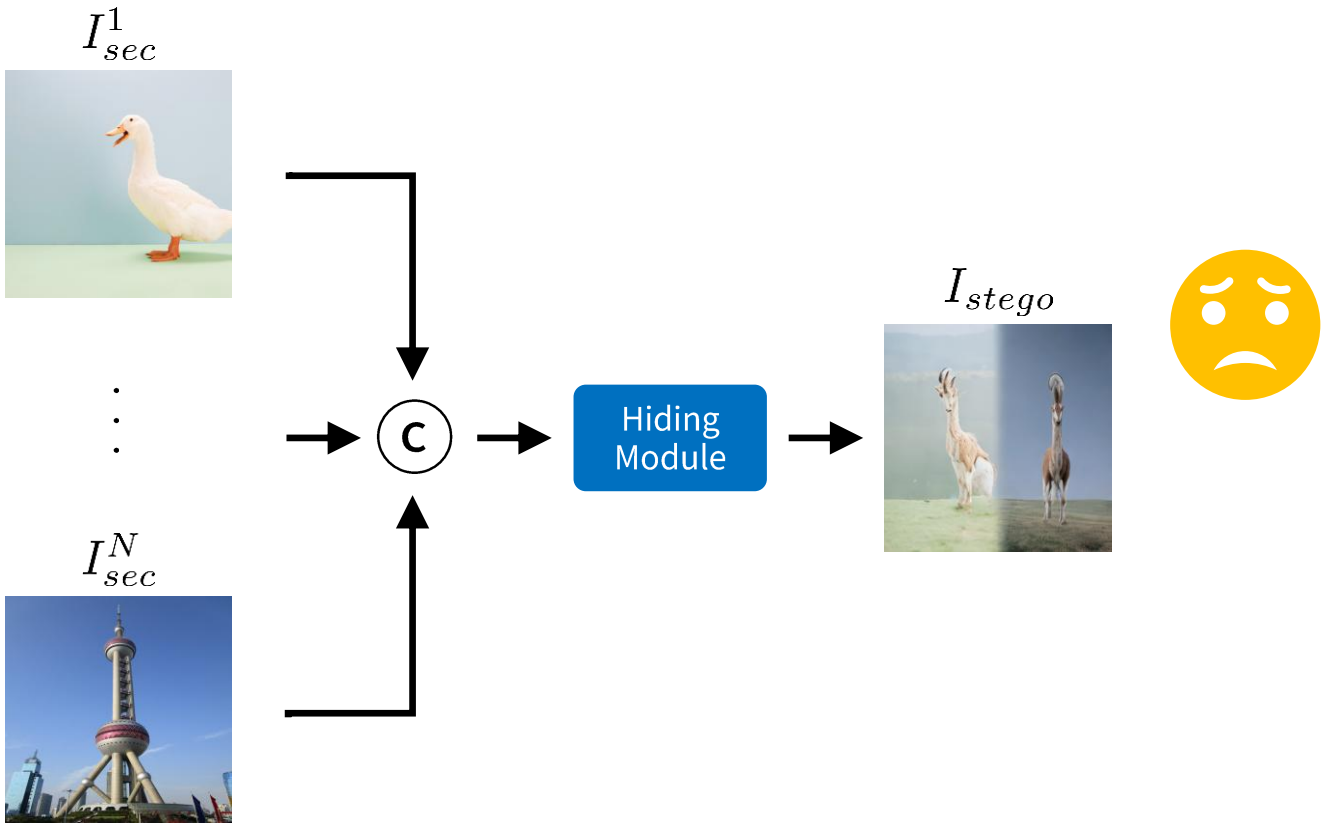
- **Training-free Coverless Multi-image Steganography with Access Control**



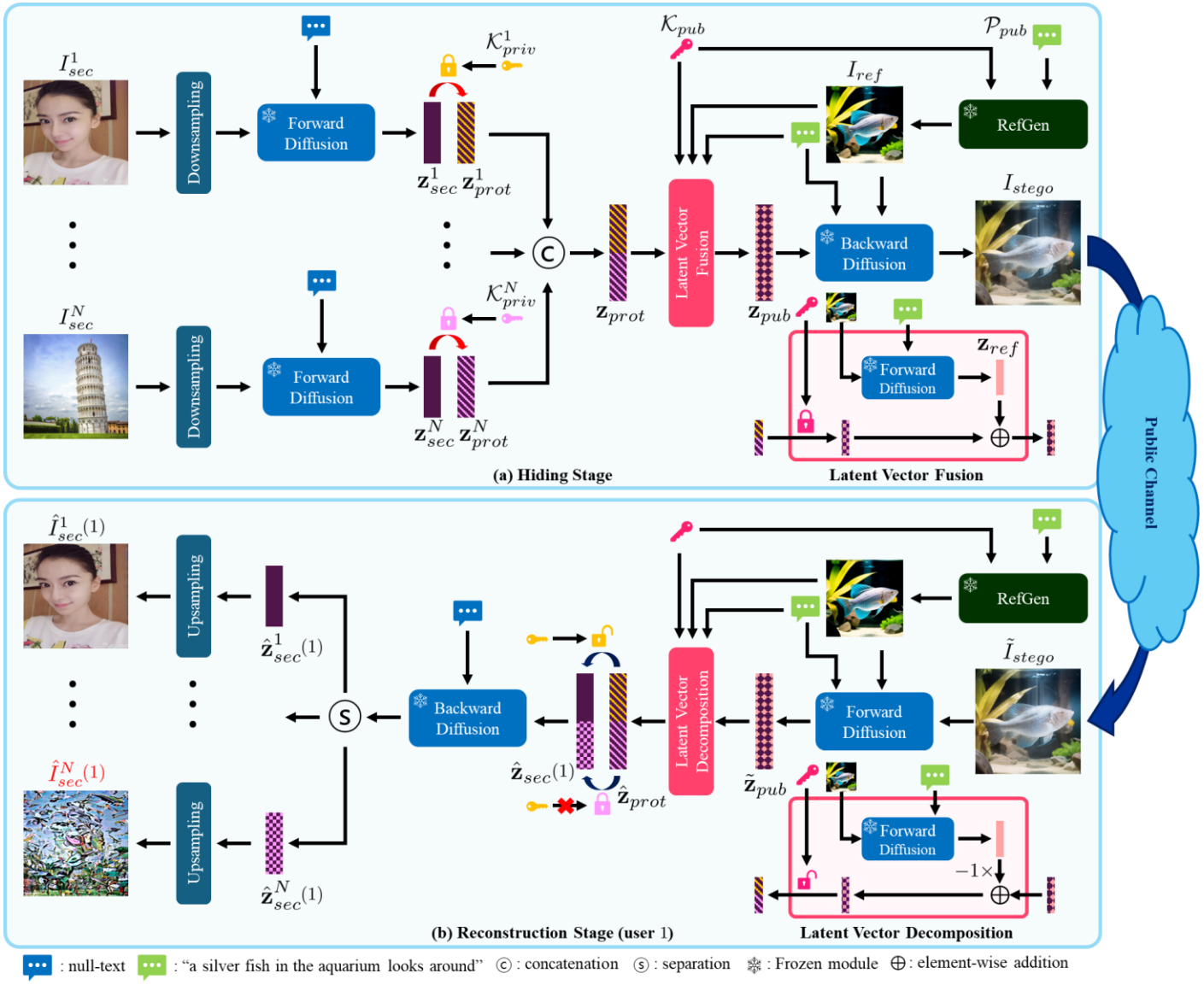
Naïve Idea: Concatenation



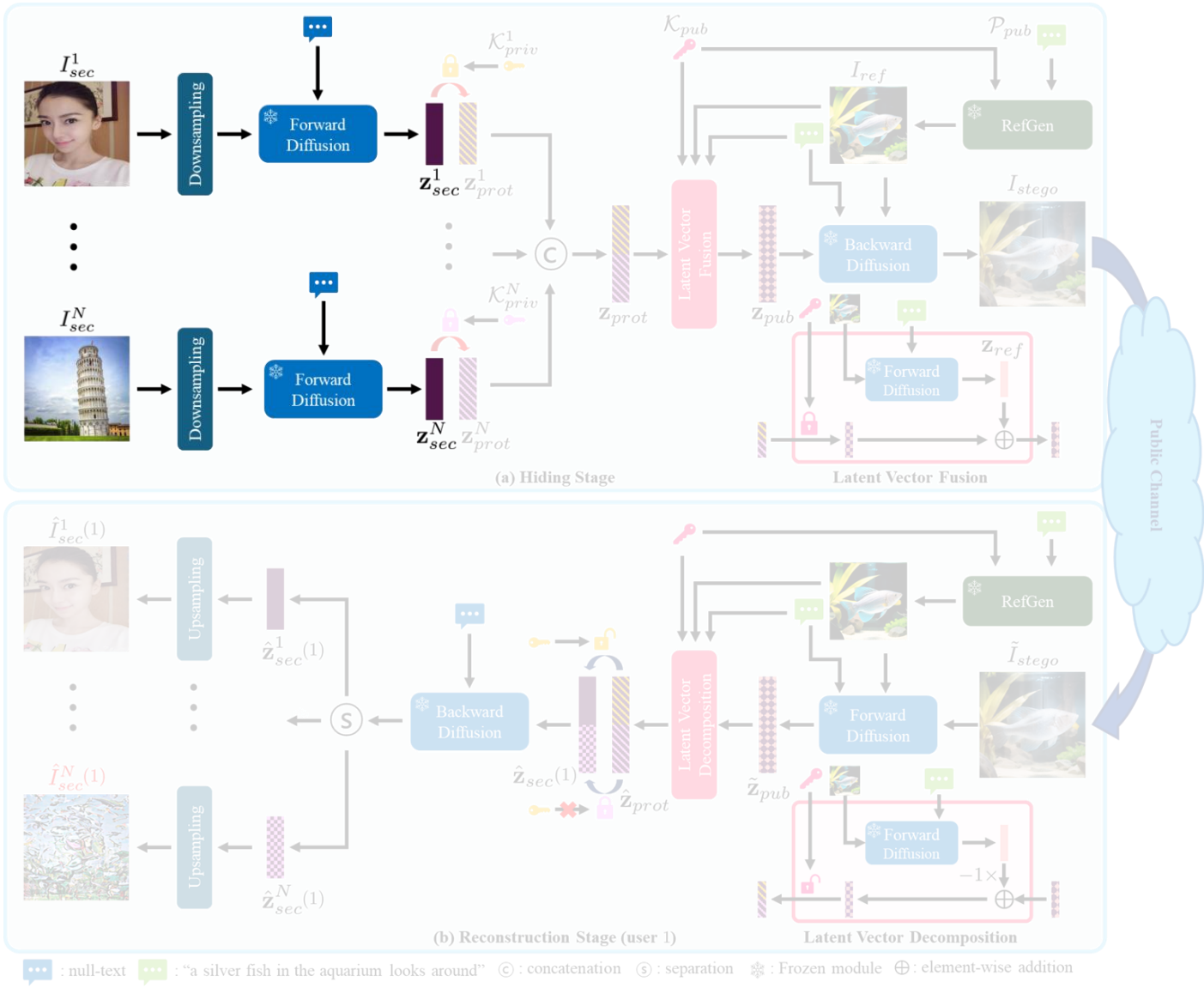
Problem: Residual Structural Patterns



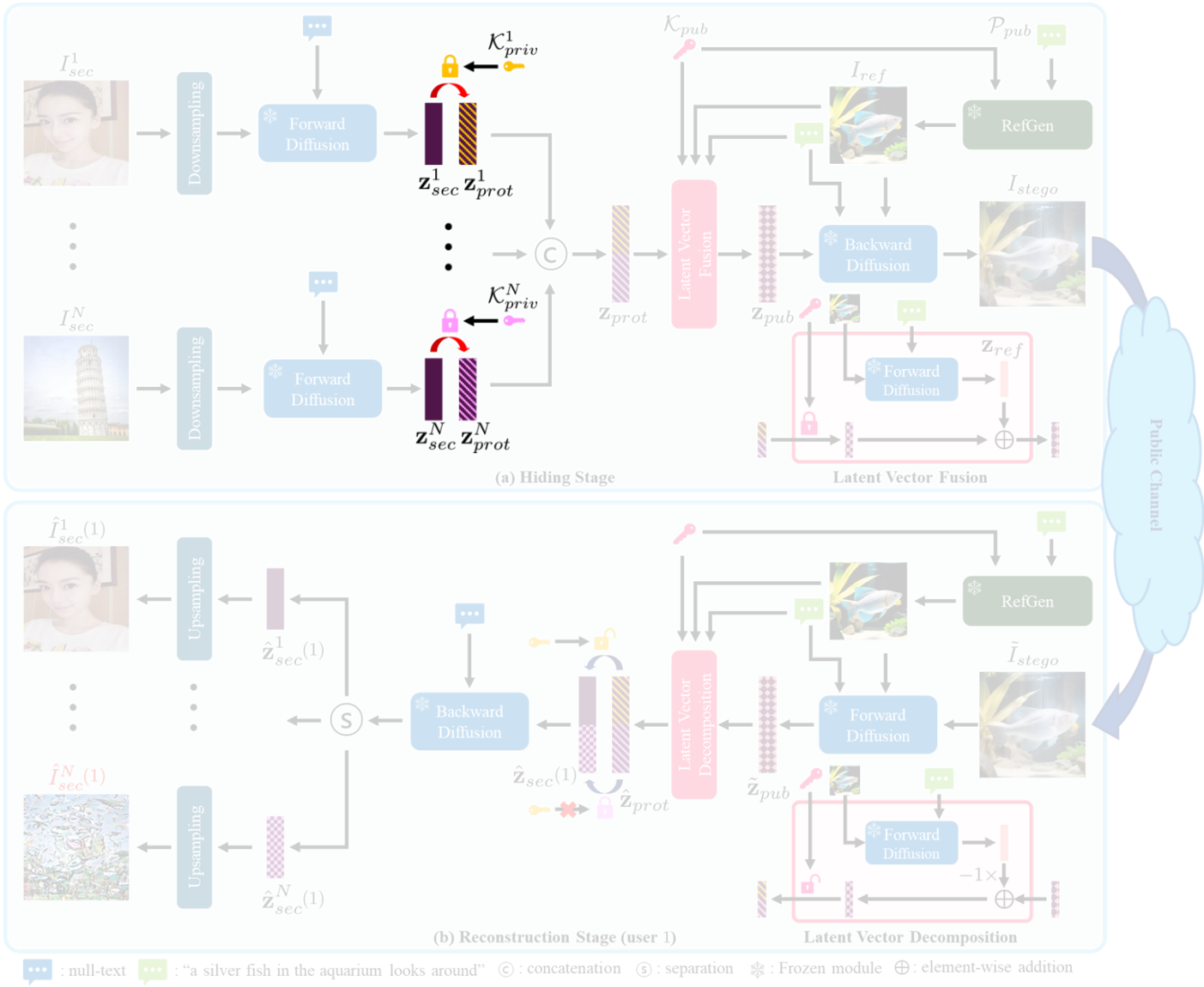
Overall Architecture



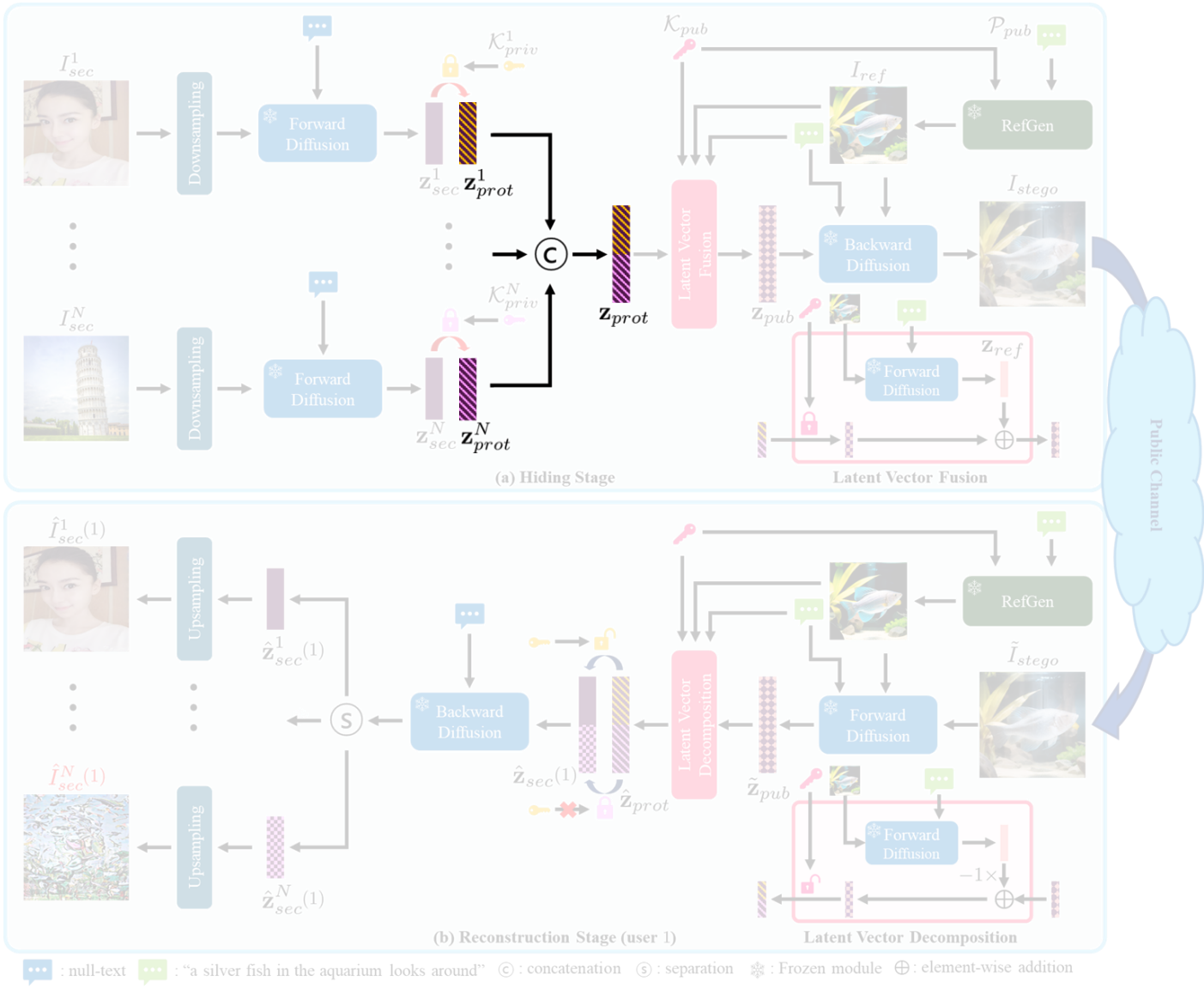
Overall Architecture



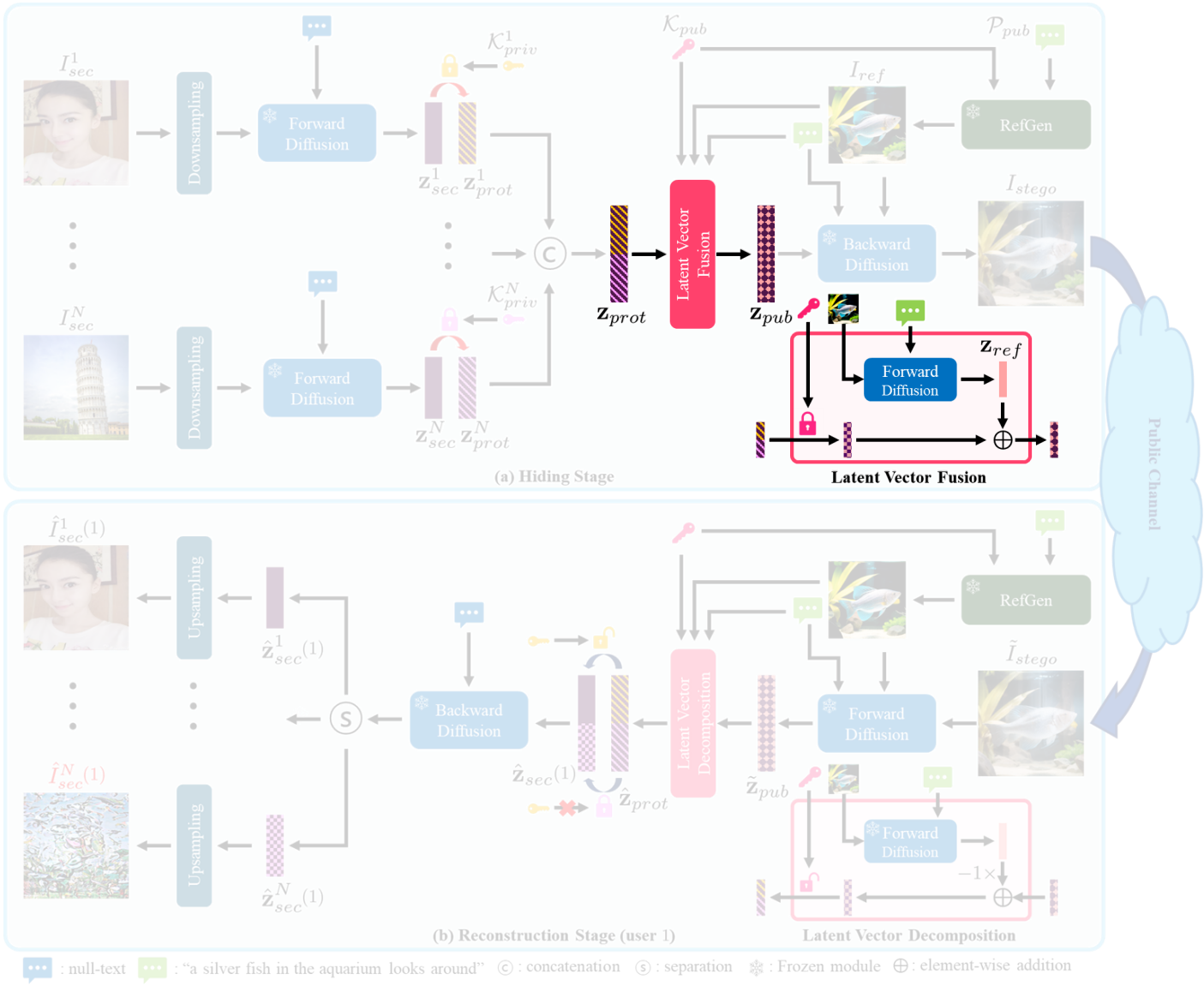
Overall Architecture



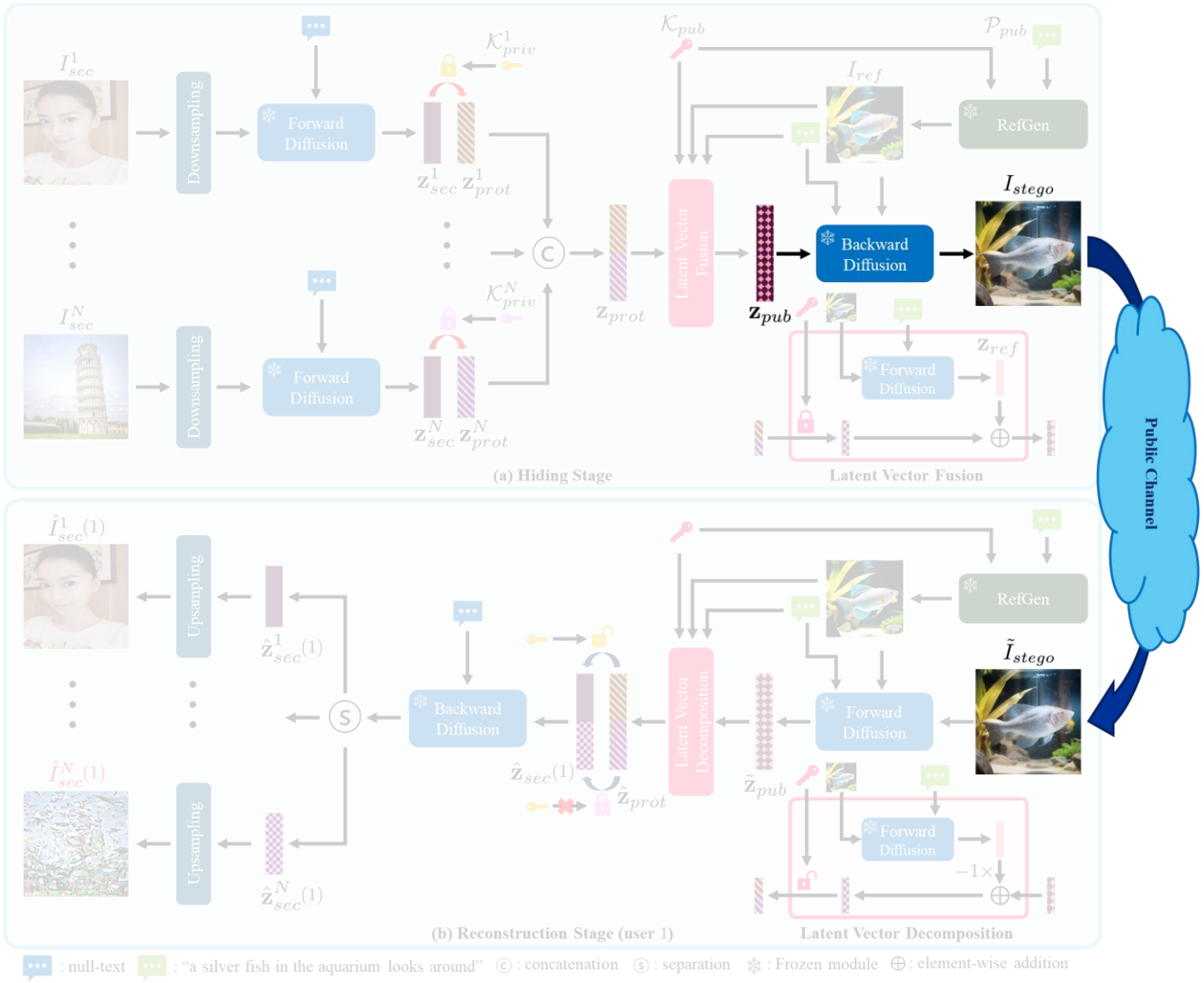
Overall Architecture



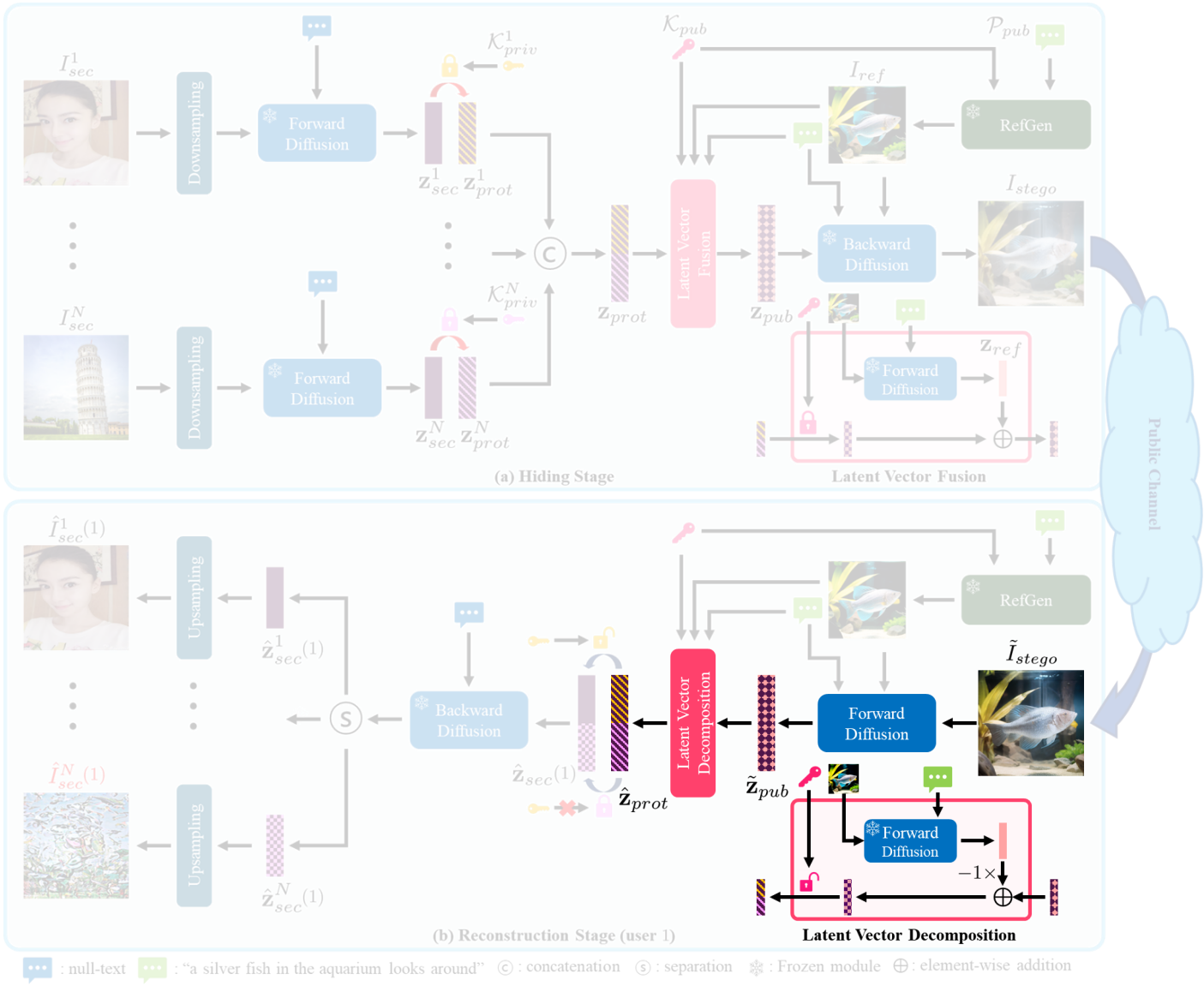
Overall Architecture



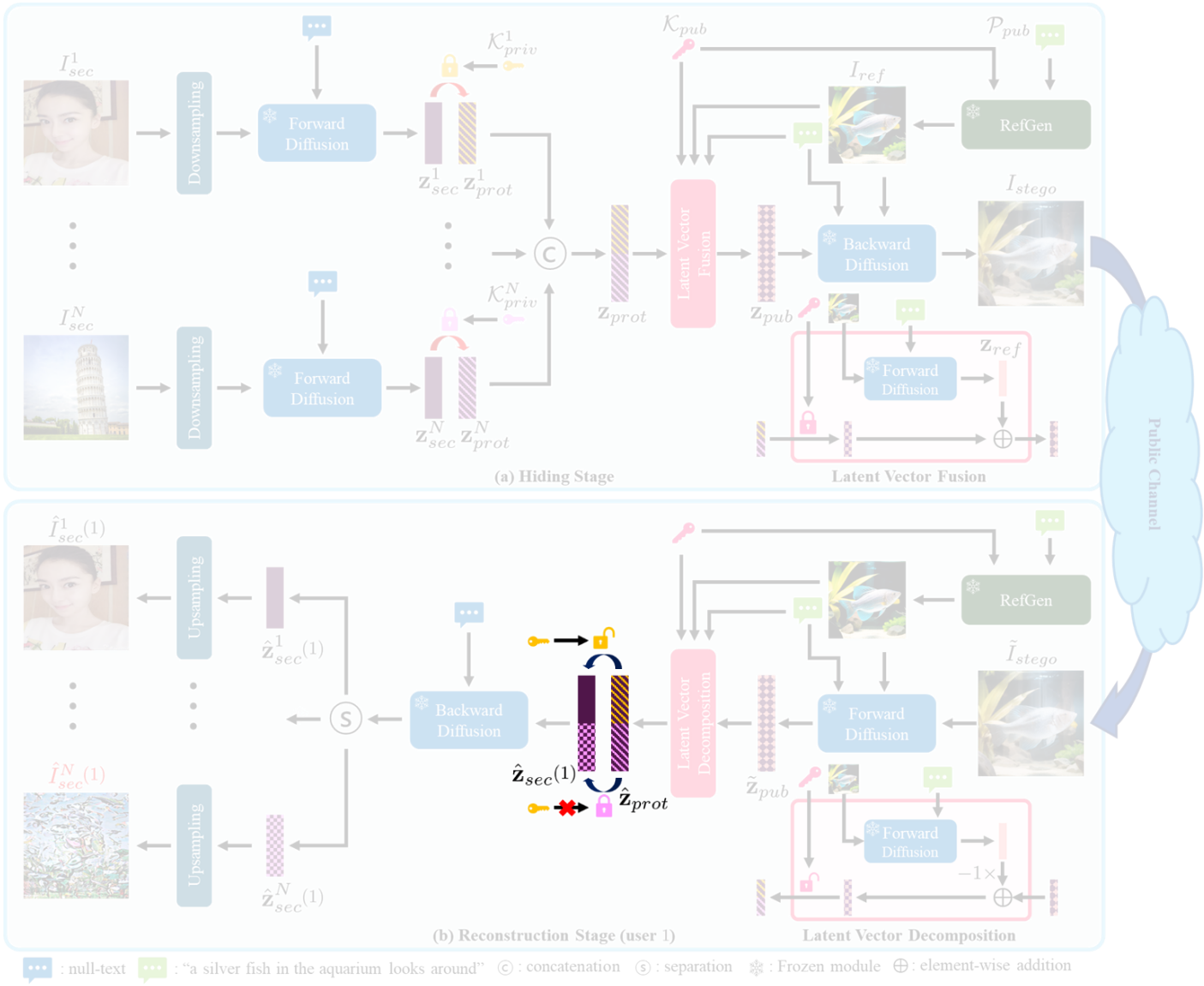
Overall Architecture



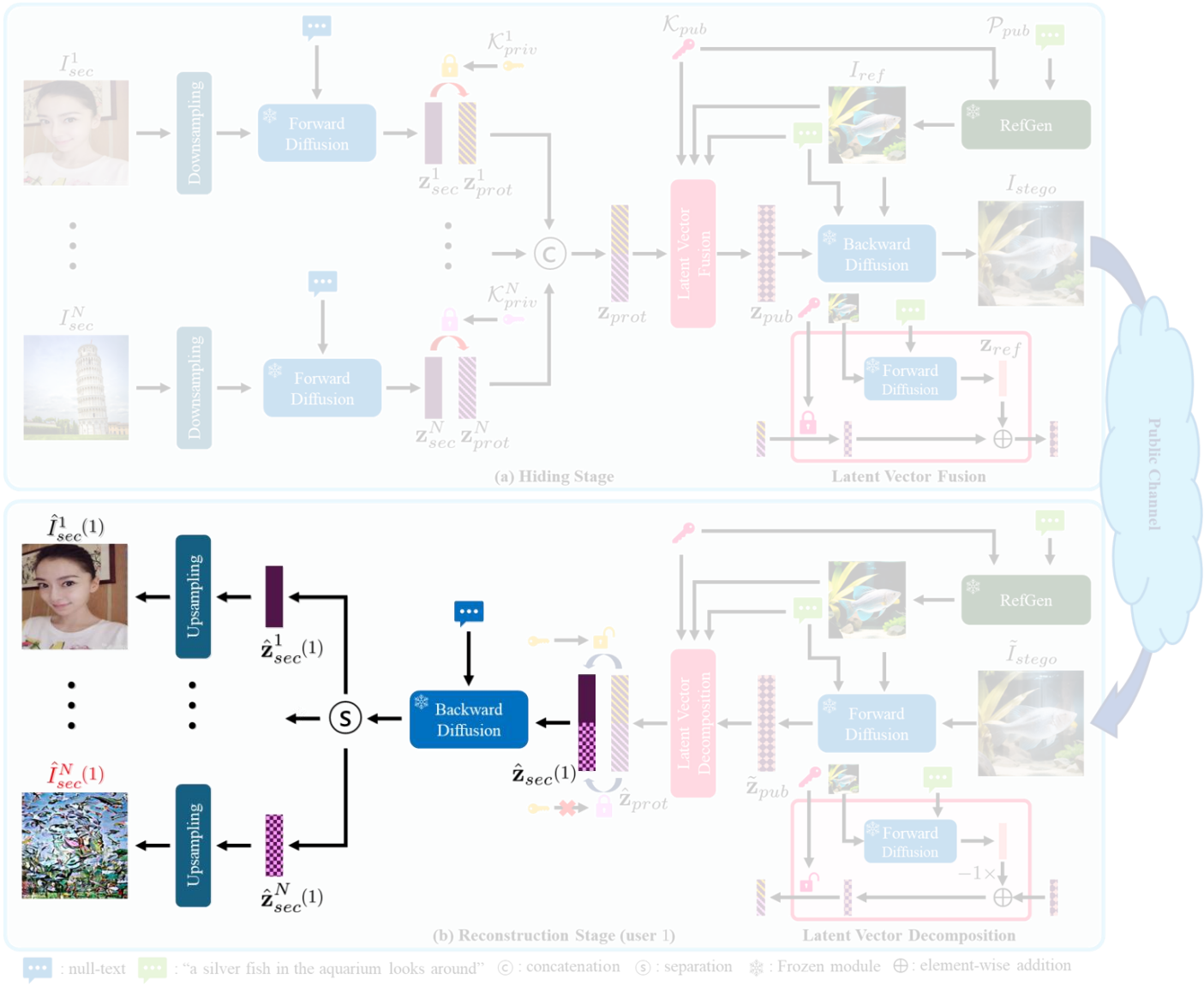
Overall Architecture



Overall Architecture



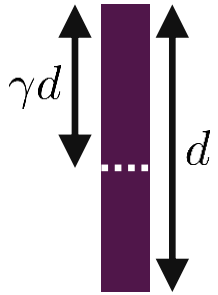
Overall Architecture



Key Components

Random Basis

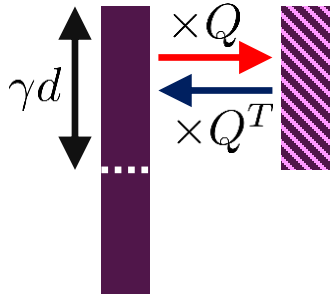
- Multiplication with an orthonormal matrix



Key Components

Random Basis

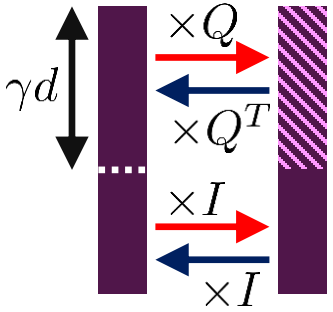
- Multiplication with an orthonormal matrix



Key Components

Random Basis

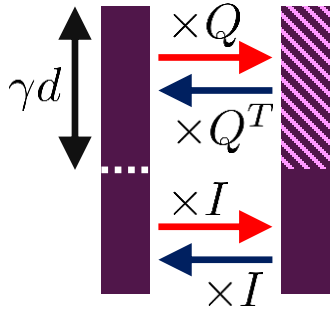
- Multiplication with an orthonormal matrix



Key Components

Random Basis

- Multiplication with an orthonormal matrix
- Security Analysis
  - Security metric: $R_L = \frac{1}{m} I(I_{sec}; \hat{I}_{sec})$
  - Main Result



Theorem 3.1. *Assume that all variables are quantized with sufficiently small step size Δ. For sufficiently large m, the information leakage under the Random Basis mechanism with strength $\gamma > 0$ satisfies*

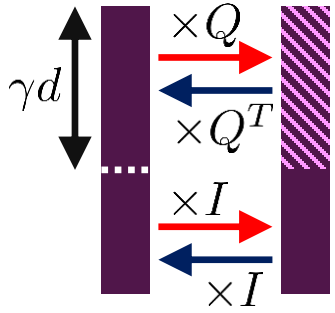
$$R_L \approx O\left(\frac{-\log \Delta + \log m}{m} + (1-\gamma)(-\log \Delta + 1)\right).$$

- ✓ In practice, the first term becomes negligible since $\Delta \approx 10^{-7}$ (float32), $m \approx 10^6$ (for a $512 \times 512 \times 3$ image).
- ✓ The second term vanishes as $\gamma \to 1$.

Key Components

Random Basis

- Multiplication with an orthonormal matrix
- Security Analysis
  - Security metric: $R_L = \frac{1}{m} I(I_{sec}; \hat{I}_{sec})$
  - Main Result



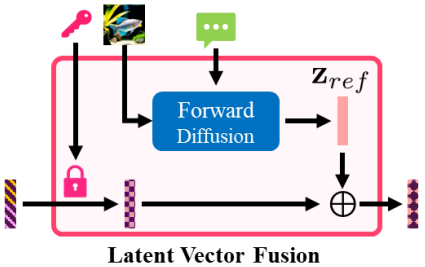
Theorem 3.1. *Assume that all variables are quantized with sufficiently small step size Δ. For sufficiently large m, the information leakage under the Random Basis mechanism with strength $\gamma > 0$ satisfies*

$$R_L \approx O\left(\frac{-\log \Delta + \log m}{m} + (1-\gamma)(-\log \Delta + 1)\right).$$

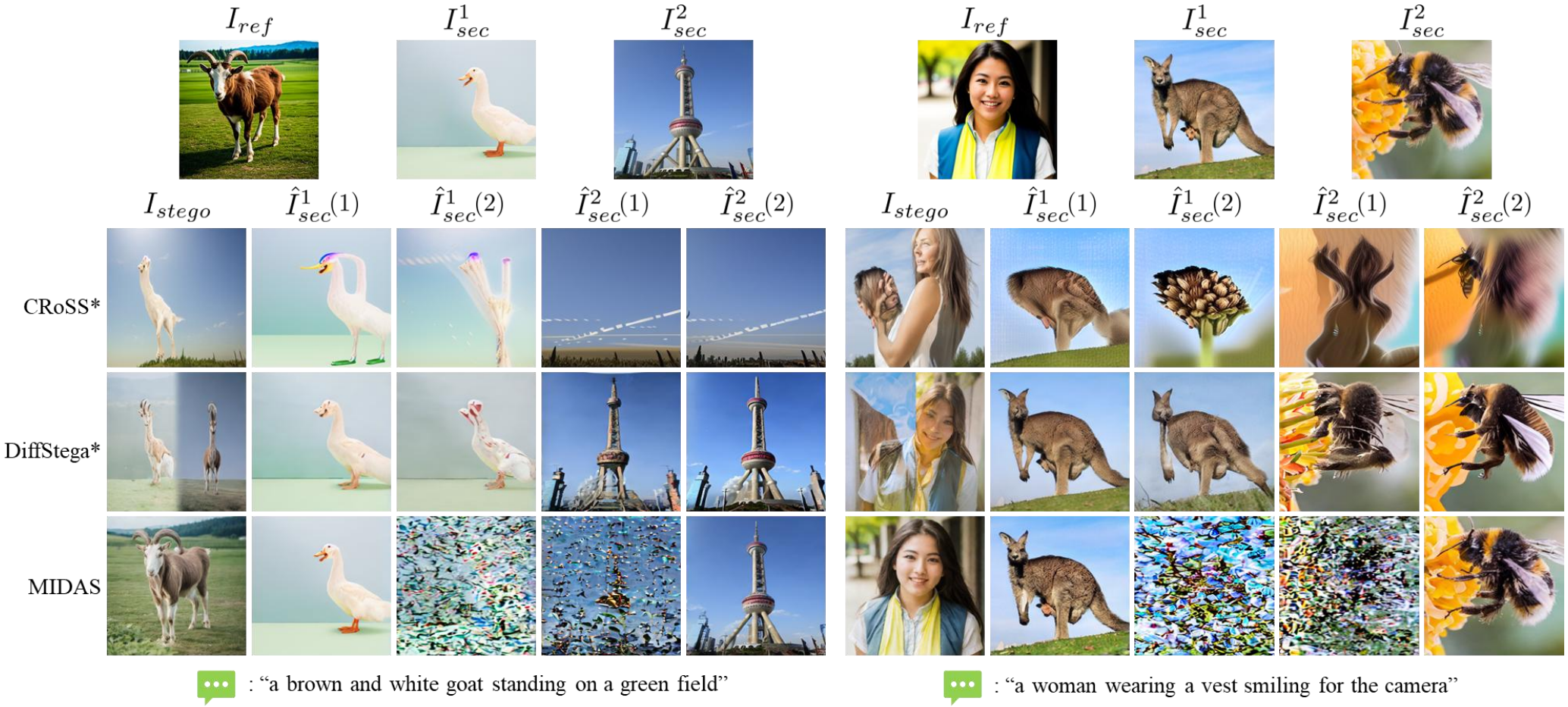
- ✓ In practice, the first term becomes negligible since $\Delta \approx 10^{-7}$ (float32), $m \approx 10^6$ (for a $512 \times 512 \times 3$ image).
- ✓ The second term vanishes as $\gamma \to 1$.

Latent Vector Fusion/Decomposition

- Shuffles concatenated secret representations.
- Injects reference information to improve generation quality.
- Uses only publicly available resources.



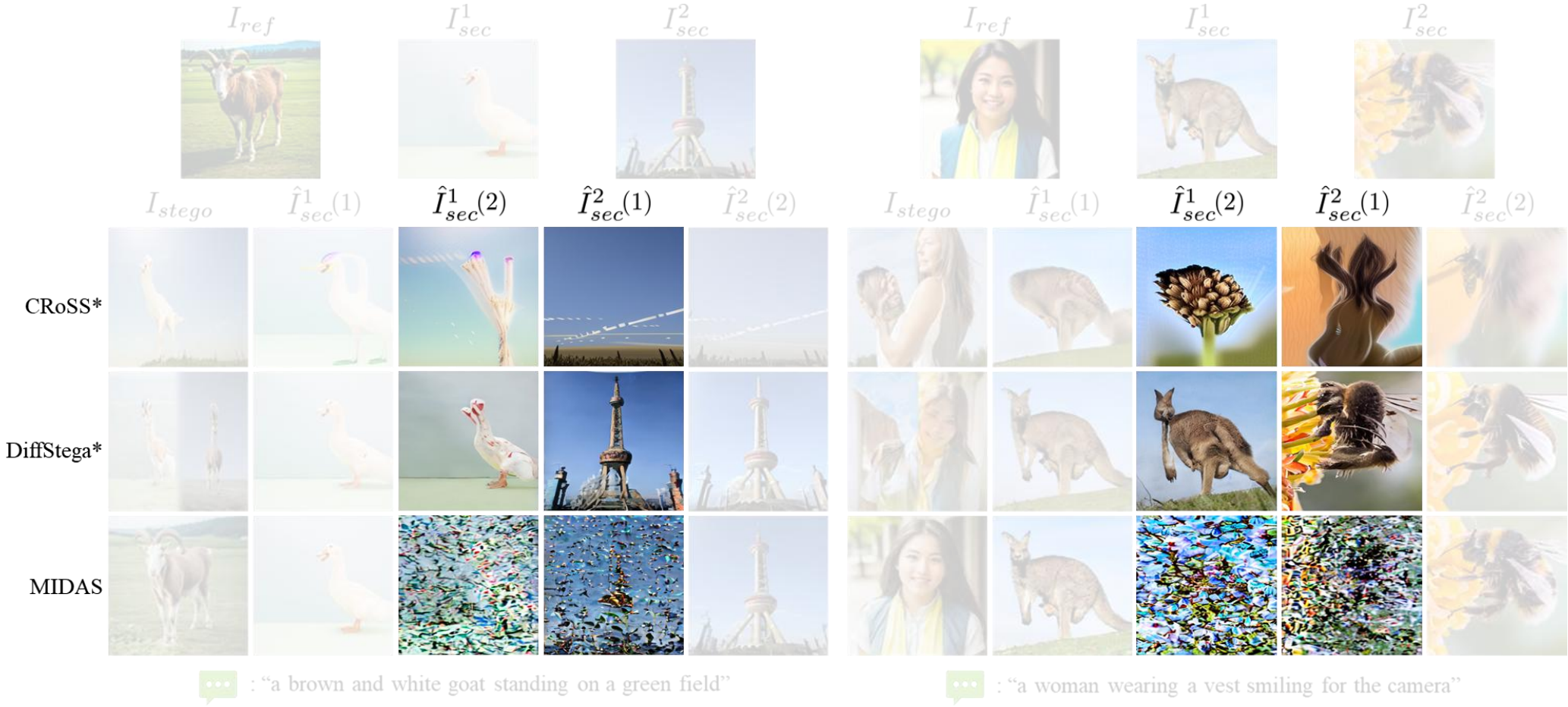
Qualitative Results



Qualitative Results

Qualitative Results

Qualitative Results



Quantitative Results

Table 2. Quantitative results for stego and reconstructed images on the Stego260 dataset. Best results among training-free CIS methods are highlighted in **bold**.

N	Method	Stego image quality	Stego image diversity				Correct $\mathcal{K}_{priv}$ reconstruction			Wrong $\mathcal{K}_{priv}$ reconstruction		
		MANIQA↑	PSNR↓	SSIM↓	LPIPS↑	CLIP Score↑	PSNR↑	SSIM↑	LPIPS↓	PSNR↓	SSIM↓	LPIPS↑
1	IIS	-	-	-	-	-	48.588	0.999	0.016	10.551	0.107	0.818
	AIS	-	-	-	-	-	35.990	0.999	0.127	22.981	0.595	0.367
	CRoSS*	0.409	20.535	0.740	0.322	27.937	22.870	0.796	0.263	18.387	0.650	0.430
	DiffStega*	**0.450**	19.686	0.664	0.419	28.871	24.958	**0.833**	**0.232**	19.447	0.650	0.397
	MIDAS(Ours)	0.429	**13.407**	**0.419**	**0.610**	**29.686**	**25.161**	0.831	0.234	**12.718**	**0.237**	**0.698**
2	IIS	-	-	-	-	-	41.360	0.995	0.070	11.883	0.219	0.808
	AIS	-	-	-	-	-	30.724	0.973	0.317	4.540	0.126	0.847
	CRoSS*	0.406	15.550	0.521	0.579	26.071	17.606	0.563	0.496	15.270	0.470	0.576
	DiffStega*	0.399	17.065	0.531	0.555	26.952	21.908	0.728	0.344	18.137	0.587	0.458
	MIDAS(Ours)	**0.434**	**9.885**	**0.287**	**0.752**	**30.129**	**23.903**	**0.771**	**0.299**	**9.964**	**0.090**	**0.753**
4	IIS	-	-	-	-	-	33.540	0.976	0.184	15.783	0.338	0.686
	AIS	-	-	-	-	-	28.045	0.956	0.369	5.131	0.126	0.947
	CRoSS*	0.418	13.445	0.453	0.687	24.601	13.190	0.312	0.681	12.731	0.297	0.696
	DiffStega*	0.364	16.160	0.509	0.600	27.367	19.233	0.609	0.442	17.533	0.545	0.508
	MIDAS(Ours)	**0.479**	**8.996**	**0.296**	**0.787**	**30.169**	**22.283**	**0.697**	**0.359**	**9.399**	**0.118**	**0.763**

Anti-Steganalysis

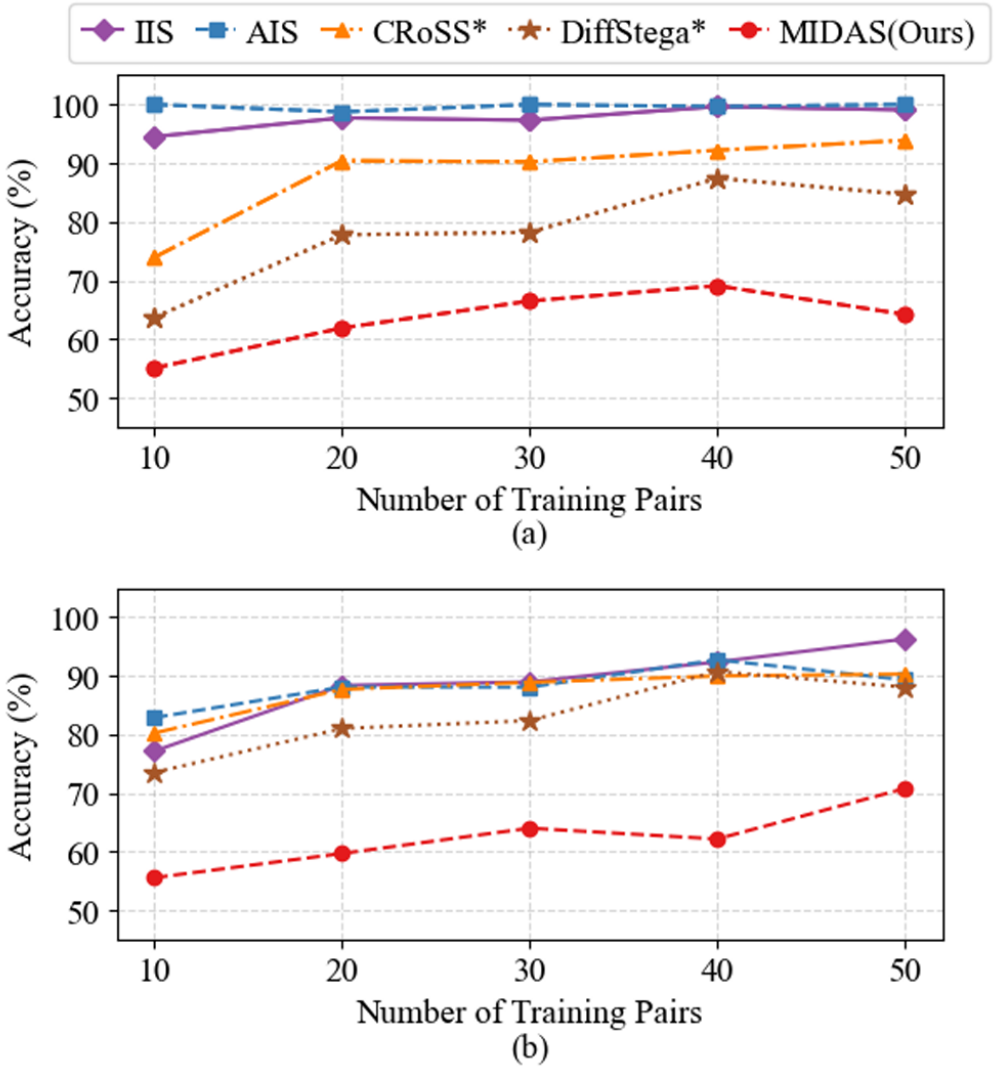


Figure 4. Steganalysis accuracy on (a) XuNet and (b) SiaStegNet.

Key Contributions

- Training-free multi-image CIS with access control
- Information-theoretic security guarantees
- Visually natural stego images with strong resistance to steganalysis

Thank you

Paper

Code